Ein Verlagsbeiheft der Heise Zeitschriften Verlag GmbH & Co. KG



extra Security

Schwerpunkt: Data Leakage Prevention

Veranstaltungen

22. – 27. Juni, Boston
Usenix Annual Technical Conference
www.usenix.org/events/usenix08

25. – 26. Juni, Berlin
D.A.CH Security
www.syssec.at/dachsecurity2008

3. Juli, Stuttgart
11. Java Forum Stuttgart 2008
www.java-forum-stuttgart.de

20. – 24. August, Leipzig
Games Convention
www.gc-germany.com

iX extra Security zum Nachschlagen:
www.heise.de/ix/extra/security.shtml

Abgedichtet

Vertrauliche Unternehmensdaten schützen

Systeme, die vertrauliche Daten im Unternehmen aufspüren und verhindern, dass sie in unbefugte Hände geraten, können einen erheblichen Beitrag zur Datensicherheit leisten. Ein sinnvoller Einsatz von Data Leakage Prevention ist jedoch nur dann gegeben, wenn Verantwortliche die juristischen, betrieblichen sowie technischen Möglichkeiten und Grenzen berücksichtigen.

Vor externen Bedrohungen schützen sich viele Unternehmen mit Firewalls, Intrusion-Prevention- und Intrusion-Detection-Systemen oder Anti-Spyware-Programmen. Die Kontrolle des Datenflusses aus dem Unternehmen heraus ist mit herkömmlichen Schutzmechanismen jedoch nicht möglich. Und obwohl es klare gesetzliche Bestimmungen zum Umgang mit vertraulichen Daten gibt, stellt ihr Schutz viele Unternehmen immer noch vor große Probleme. So musste die Bundesregierung im März dieses Jahres eingestehen, dass seit Januar 2005 rund 500 Notebooks und PCs aus Bundesbehörden verschwanden.

Es stellt sich die Frage, ob Unternehmen ihre sensitiven Daten überhaupt effektiv gegen Verlust schützen können. Denn erlangt ein autorisierter Anwender Zugriff auf sie, hat er in den meisten Fällen erst einmal freie Hand. Er kann Daten kopieren, ausdrucken oder einfach per E-Mail verschicken – und somit auch verlieren oder stehlen. Die Auswirkungen: Verlust geistigen Eigentums, schwindendes Kundenvertrauen, rechtliche Konsequenzen. Um solcherlei Schaden abzuwenden, suchen immer mehr Organisationen nach praktikablen Ansätzen. Eine neue „Zauberformel“ namens Data Loss (oder Leakage) Prevention, kurz DLP, soll ihnen helfen, die Nutzung und Verbreitung ihrer Firmendaten zu überwachen und zu kontrollieren.

DLP – ein Kind mit vielen Namen

Der Schutz vor Datenverlusten durch autorisierte Benutzer wird von den Herstellern inzwischen fast ausnahmslos durch eigene Begrifflichkeiten umschrieben. Information Leak(age) Prevention, Information Leak Detection and Prevention, Data Extrusion Prevention, Content Monitoring and Filtering, Extrusion Detection, Outbound Content Compli-



„Compliance Summary Dashboard“: In der Übersicht des DLP-Produkts von Lumension kann der Systemverantwortliche den Status aller angeschlossenen Endgeräte betrachten (Abb. 1).

ance oder Insider Threat Protection – all diese Techniken haben das Ziel, vertrauliche Daten im Unternehmen aufzuspüren und unter Kontrolle zu halten. Am häufigsten anzutreffen sind jedoch die – daher im Folgenden verwendeten – Begriffe Data Loss oder auch Data Leakage Prevention (DLP).

Eine Untersuchung der verfügbaren Produkte bringt schnell an den Tag, dass nicht überall, wo DLP draufsteht, auch DLP drin ist. Meist finden sich nur Teilaspekte einer solchen Lösung. So setzen die Hersteller etwa auf Verschlüsselung der Daten auf Festplatten oder Mobile Devices, Anwendungen zur Kontrolle von Wechselmedien oder Mailverschlüsselungs-Gateways zum Schutz vertraulicher Informationen. Andere konzentrieren sich auf E-Mail-Gateways und Web-Proxies zur Analyse der im Netz übertragenen Inhalte, um darin enthaltene vertrauliche Daten zu entdecken und gegebenenfalls Schutzmaßnahmen einzuleiten.

Eine „echte“ DLP-Lösung jedoch sollte den Anwender mit Zugriff auf sensitive Daten an einer unsachgemäßen Nutzung hindern. Dazu muss die Software in der Lage sein, anhand verschiedener Kriterien zwischen vertraulichen und nicht vertraulichen Daten zu unterscheiden. Zu der benötigten Funktion gehört die genaue Analyse der Inhalte, das Wissen um ihren Speicherort sowie die Fähigkeit, Daten in ihrer Beziehung zueinander, also ihrem Kontext zu erkennen.

Zwei technische Ansätze

Im Wesentlichen gibt es bei DLP-Lösungen zwei unterschiedliche technische Ansätze, den netzwerk- und den hostbasierenden. Netzwerkbasierende Lösungen sind einfach zu implementieren und decken in der Regel alle gängigen Protokolle wie HTTP, HTTPS, SMTP, POP3, und IMAP ab. Sie schützen das gesamte Unternehmensnetz, bieten jedoch keinen Schutz für Wechselmedien, Screenshots oder Copy&Paste-Vorgänge auf dem Client. Technisch werden netzwerkbasierte DLP-Produkte als Application Level Proxies oder Sniffer eingesetzt. Die zweite Variante erlaubt in der Regel nur das Aufspüren kritischer Vorgänge, kann diese jedoch im Gegensatz zu den auf Applikationsebene arbeitenden Proxies nicht verhindern.

Hostbasierende Lösungen erfordern einen auf dem zu

So schützen Unternehmen ihre Daten

Risiken bewerten

Am Beginn eines jeden Projektes sollte immer eine Bestandsaufnahme in Verbindung mit einer Risikoanalyse stehen: Welche Daten sind zu schützen, wo liegen sie und wie sehen die Sicherheitsbestimmungen aus, die diese Informationen schützen? Im Rahmen einer Risikobewertung ist festzustellen, wo die wichtigsten Gefahrenquellen (etwa Mobile Devices, Web oder E-Mail) für einen Datenverlust lauern. Danach folgt eine entsprechende Priorisierung der Gefährdungswahrscheinlichkeiten. Dies gibt der IT-Abteilung Hinweise, wo und mit welchen DLP-Komponenten die Hebel anzusetzen sind.

Flexibel gestalten

Den Anforderungen und Sicherheitsbestimmungen eines Unternehmens entsprechend gilt es, das DLP-Produkt so umfassend und flexibel wie möglich zu gestalten. Zu beachten sind besonders Funktionen wie eine umfassende Überwachung und Absicherung der verwendeten Protokolle, aber auch eine inhaltsbasierende Analyse aller sensitiven Dokumenten- und Attachment-Typen. Nachrichten mit vertraulichen Inhalten an unberechtigte Empfänger sollten isoliert und blockiert werden. Außerdem ist eine umfassende und automatisierte Verschlüsselung der Daten gemäß der Sicherheitsrichtlinien des Unternehmens durchzusetzen.

Handlungsfähigkeit erhalten

Ein gutes DLP-Produkt sollte skalierbar sein und sich dynamisch den wechselnden Gegebenheiten und Anforderungen im Unternehmen anpassen können, ohne dass dies zu Lasten einer effektiven Kommunikation oder des Schutzes vertraulicher Daten geht. Hierzu bedarf es akkurat ausformulierter Regelungen und klar definierter Prozesse für das Überwachen sämtlicher Kommunikationswege im Unternehmen wie E-Mail, Instant Messaging, Webmail oder Webformulare.

Informationen gewinnen

Um den zunehmenden Compliance-Anforderungen gerecht zu werden, sollte ein DLP-Produkt als Bestandteil eines Security-Information-Managements einfach zu verwalten sein, Archivierungsmöglichkeiten bieten und ein detailliertes Reporting über eventuelle Sicherheitsvorfälle ermöglichen. Denn nur durch ein ausführliches Berichtswesen erhalten die verantwortlichen Mitarbeiter alle notwendigen Informationen beispielsweise zu Absender und Empfänger der Daten oder den Inhalten von Anhängen und können so im Idealfall bereits präventiv Gefahren fürs Unternehmen abwehren.

An den Nutzer denken

Auch im beruflichen Alltag gibt es immer mehr unverwaltete Handhelds, PDAs, USB-Sticks oder Software. Zusätzlich lauern die Gefahren in der zunehmenden Nutzung von E-Mail zu privaten Zwecken, Blogging oder Instant Messaging am Arbeitsplatz. Entsprechende Nutzungsrichtlinien mit klar definierten Formulierungen helfen hier, das Risiko gering zu halten. Auch sollten sich die Richtlinien an der täglichen Praxis orientieren und einen ausgewogenen Mix zwischen Wahlfreiheit und Sicherheit für die unterschiedlichen betrieblichen Anforderungen gewährleisten. Man darf den Anwender in seinen Arbeitsabläufen nicht behindern und muss den unterschiedlichen Arbeitsprozessen aller Abteilungen den nötigen Spielraum lassen. Ein geeignetes Instrument zur Durchsetzung dieser Policies ist ein schriftlicher Sicherheitsfaden, der von jedem Mitarbeiter zu unterzeichnen ist.

Vertrauliche Daten müssen auch vertraulich bleiben - der Schlüssel zur maximalen Datensicherheit

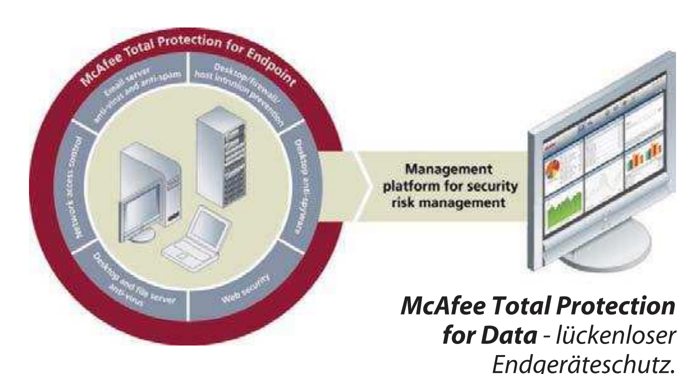
Das *Risiko personenbezogene und vertrauliche Daten zu verlieren* nimmt stetig zu, lässt sich aber effektiv vermeiden – mit Data Protection-Lösungen der neuesten Generation.

Obwohl es seit Jahren gesetzliche Vorschriften zum Datenschutz gibt, stellt der Verlust von Unternehmensdaten immer noch ein Problem dar. Egal, ob Informationen aus Versehen oder durch vorsätzliche Aktivitäten verlorengehen oder weitergegeben werden, der Schaden kann oft erhebliche Ausmaße annehmen.
Im spektakulärsten Fall sind beim britischen Verteidigungsministerium persönliche Daten, darunter Namen, Adressen, Bankverbindungen und Familienstand, von mehr als 600.000 Rekruten oder Militärdienstanwärtern abhanden gekommen. Ein Mitarbeiter des Ministeriums hatte diese Daten auf einem Notebook gespeichert, das gestohlen wurde.

Dieser Fall zeigt ein weiteres Mal, dass die derzeit üblichen Maßnahmen den Verlust oder die Weitergabe von Daten nicht abdecken. Der traditionelle Ansatz zur Datensicherheit konzentriert sich darauf, durch Firewalls, Intrusion Prevention, Spyware-Schutz und Datenverschlüsselung „die Übeltäter draußen zu halten". Um den nicht autorisierten Zugriff auf Informationen durch Insider zu kontrollieren, verwenden viele Unternehmen Identitäts-Management-Systeme und Zugangskontrolllisten. Diese sind zwar nützlich, schützen ein Unternehmen aber nicht ganzheitlich vor unberechtigtem Zugriff auf vertrauliche Daten. Alle diese Ansätze lassen Sicherheitslücken offen: in Form von unbeabsichtigtem Verlust oder vorsätzlicher Weitergabe von Daten durch autorisierte Benutzer.

Um alle Risiken des Datenverlusts abzuwenden, müssen Unternehmen Inhalte über deren gesamten Lebenszyklus hinweg überwachen. Vertrauliche Daten werden oft auf zentralen Servern gespeichert, aber auch von autorisierten Benutzern erstellt, verändert, ausgedruckt und kopiert. Sie werden gemeinsam genutzt – als Ausdruck, auf USB-Laufwerken und über Netzwerke. Nach der Bearbeitung werden sie von Benutzern auf einer lokalen Festplatte, durch Speicherung auf CD-ROM oder einem USB-Stick, als Ausdruck in Akten oder durch Versenden im Netzwerk archiviert. Ein vollständiger Schutz muss diese legitimen Nutzungsarten und Erfordernisse sowie die organisatorischen Grenzen, etwa Intranets für Buchhaltung und Marketing oder die öffentlich zugängliche Webseite, berücksichtigen. Der richtige Ansatz ermöglicht eine adäquate geschäftliche Bearbeitung und zeitgerechte gemeinsame Nutzung von Daten innerhalb und außerhalb des Unternehmens.

McAfee® Total Protection for Data zielt exakt auf die beschriebene Problematik ab und ist branchenweit die kompletteste Lösung zum Schutz vertraulicher Daten.



***McAfee Total Protection for Data** - lückenloser Endgeräteschutz.*

Mit dieser Lösung reagiert McAfee auf die Ausweitung der Rechtsvorschriften, die Unternehmen im Umgang mit Kundendaten zu beachten haben. Das Besondere daran ist die Kombination aus effizienter Netzwerkadministration und detaillierter Endgeräteüberwachung mit einem einzigen Datenschutz-Management-System.

Schutz von Daten vor nicht autorisierter Weitergabe

Mit McAfee Host Data Loss Prevention können Sie unternehmensweite Sicherheitsrichtlinien aufstellen und durchsetzen, die Ihren Mitarbeitern Regeln und Beschränkungen für die Verwendung von sensiblen Daten sowie für die Datenübertragung auf gängigen Wegen wie E-Mail, Instant Messenger, Druck oder USB-Laufwerke vorgeben. Ob Ihre Mitarbeiter am Arbeitsplatz, zuhause oder unterwegs sind, spielt dabei keine Rolle - die Kontrolle bleibt in Ihren Händen.

Verschlüsselung ganzer Festplatten

Mit McAfee Endpoint Encryption kommen eine strenge Zugangskontrolle mit Anwender-Authentifizierung noch vor dem Hochfahren des Betriebssystems (Pre-Boot-Authentifizierung) und staatlich zertifizierte Verschlüsselungsalgorithmen zum Schutz von Daten auf Endgeräten wie Desktops, Laptops, Tablet-PCs, Smartphones und PDAs zum Einsatz. Ver- und Entschlüsselung sind für den Anwender transparent, finden bei laufendem Betrieb statt und haben so gut wie keinen Leistungsverlust zur Folge.

Verschlüsselung von Dateien und Ordnern

Bestimmen Sie, welche Dateien oder Ordner verschlüsselt werden. Mit McAfee Endpoint Encryption können Administratoren die Verschlüsselung der Inhalte bestimmter Ordner sowie von Dateien aus bestimmten Anwendungen oder eines bestimmten Dateityps festlegen. Anwendergruppen erhalten selektive Zugriffsrechte auf bestimmte Dateien und Ordner und können diese über das gesamte Netzwerk hinweg sicher gemeinsam nutzen. Egal, wo Dateien gespeichert sind oder wohin sie übertragen werden, die Daten bleiben dank der Persistent Encryption Technology™ stets verschlüsselt. Wenn ein unbefugter Anwender versucht, eine Datei, die auf einem Firmenlaptop einsehbar ist, auf einem nicht genehmigten Gerät zu speichern, so erhält er nur eine verschlüsselte und damit unlesbare Datei.

McAfee®

Ohmstraße 1
85716 Unterschleißheim
Telefon: +49 (0)89 3707 0
www.mcafee.com/de



DLP-Produkte findet man gelegentlich auch in Form der beliebten Hardware-Appliances (Abb. 2).

kontrollierenden Client installierten Agenten. Die vom Agenten umzusetzende Policy definiert der Systemverantwortliche auf einer zentralen DLP-Managementkonsole. Da der Agent selbst auf dem Client arbeitet, kann er grundsätzlich alle dort stattfindenden Aktionen reglementieren. Im Vergleich zu netzwerkbasierten Lösungen lassen sich so weiterreichende Schutzmaßnahmen umsetzen.

Auch die Anwenderbenachrichtigung im Fall eines Regelverstoßes kann unmittelbar und aussagekräftig durch vom Agenten auf dem Client generierte Pop-up-Warnmeldungen geschehen. Da der Agent überdies außerhalb des Unternehmensnetzes aktiv ist, sind damit ebenso remote arbeitende Laptops geschützt. Diesen Vorteilen stehen jedoch einige Nachteile gegenüber: Der Betrieb ist deutlich aufwendiger als der einer netzwerkbasierten Lösung, da die Agenten ausgerollt und aktualisiert werden müssen. Oft stehen auch nicht für alle im Unternehmen eingesetzten Betriebssysteme Agenten zur Verfügung.

Die meisten Hersteller unterscheiden hier nach „Data in Motion“, also solchen, die transportiert werden, „Data at Rest“, den gespeicherten, sowie „Data in Use“, Daten, die in Bearbeitung sind. Data in Motion sind Daten, die über das Netzwerk transportiert werden, beispielsweise per E-Mail, per HTTP in Webforen sowie per FTP oder Instant Messaging. Die Übertragung von Daten über diese Standardprotokolle lässt sich mit netzwerkbasierten Produkten kontrollieren.

Die Integration in vorhandene Web-Sicherheitsumgebungen erfolgt über eine ICAP-Anbindung (Internet Content Adaption Protocol) oder als kaskadierter Proxy. Für SMTP bindet der Systemverantwortliche die Produkte als zusätzliches Mail Relay in die Mail-Kette ein. In diesen Konfigurationen können die netzwerkbasierten DLP-Lösungen vertrauliche Inhalte nicht nur erkennen, sondern deren Übertragung auch verhindern. Eine weitere Möglichkeit besteht in einem passiven Monitoring der Netzwerkkanäle an Mirror-Ports in der Switch-Infrastruktur. Die Übertragung der Inhalte lässt sich so zwar nicht unterbinden, aber entdecken und loggen. Im Schadensfall dient sie der Beweissicherung.

Die vertraulichen Daten eines Unternehmens finden sich an unterschiedlichen Stellen. Data at Rest lagern auf zentralen Systemen wie Dateiservern, Datenbanken, Dokumentenmanagement- und Warenwirtschaftssystemen oder liegen auf Arbeitsplatzrechnern in Form lokaler Kopien, durch Kopieren erzeugter Teildokumente, E-Mail-Anhängen und vielem mehr. Während man die Daten auf zentralen Systemen gut sichern kann, ist dies auf Arbeitsplatzrechnern oft nicht der Fall. Deshalb ist es wichtig, auf diesen weniger sicheren Systemen die vertraulichen Daten ausfindig zu machen.

Zu diesem Zweck durchsuchen DLP-Produkte Fileserver, Datenbanken und andere Systeme. Um auch große, über WAN (Wide Area Network) verbundene Netze und Datenbestände in akzeptablen Zeiträumen durchsuchen zu können, verteilt eine DLP-Managementkonsole die Suchaufgabe auf dedizierte Scanning-Systeme und Software-Agenten, die jeweils Teilbereiche des Unternehmensnetzes durchsuchen und die Ergebnisse an die Konsole zurückmelden. Diese Scans erfolgen automatisch und in regelmäßigen Abständen. Aus Performancegründen werden jedoch nur inkrementelle Scans durchgeführt: Die Scanner merken sich einfach bereits gescannte Daten und durchsuchen sie nicht jedes Mal aufs Neue.

Unter Data in Use (Daten in Bearbeitung) fällt die Kontrolle der Bearbeitung der vertraulichen Daten auf dem Client. Diesen Schutz können nur hostbasierte Produkte bieten. Sie sollten neben den offensichtlichen Wegen des Daten-

HERSTELLER VON DLP-PRODUKTEN

Die folgende Übersicht hat keinen Anspruch auf Vollständigkeit.

Hersteller	Produkt	Website
Bigfix	Data Leak Prevention	www.bigfix.com
Code Green Networks	Content Inspection	www.codegreennetworks.com
CTH Technologies	SecureCare, V2.0	www.cthtech.com
EagleEyeOS	EagleEyeOS	www.eagleeyeos.com
EMC	RSA Data Loss Prevention Suite	www.rsa.com
Fidelis Security	Extrusion Prevention System	www.fidelissecurity.com
Infowatch	Infowatch	www.infowatch.com/de
Ironport	Ironport Data Leakage	www.ironport.com
itWatch	DeviceWatch, PDWatch, XRayWatch	www.itwatch.de
Lumension	Sanctuary	www.lumension.com
McAfee	Host Data Loss Prevention	www.mcafee.com/de
Mobilegov	Device Authenticator Pro	www.mobilegov.com
Oakley Networks	SureView	www.oakleynetworks.com/
Palisade	PacketSure	www.palisadesys.com
PGP	PGP Endpoint	www.pgp.com/de
Proofpoint	Proofpoint 5.0	www.proofpoint.com
Reconnex	iGuard	www.reconnex.net
Safend	Safend Auditor und Protector 3.3	www.safend.com
Symantec	Vontu Data Loss Prevention	www.symantec.de
Tizor	Mantra	www.tizor.com
Trend Micro	Leakproof 3.0	www.trendmicro.de
Utimaco	SafeGuard LeakProof	www.utimaco.de
Verdasys	Digital Guardian	www.verdasys.com
Vericept	Data Loss Prevention Solution	www.vericept.com
Websense	Intelligent Content Protection	www.websense.com/global/de/

verlustes über USB-, Wireless-LAN-, Bluetooth und Netzwerkschnittstellen auch andere kritische Benutzerhandlungen kontrollieren. Insbesondere Screenshots, Copy&Paste-Aktionen, bei denen ein Nutzer Daten aus einem geheimen Dokument etwa in eine Mail kopiert, und der Ausdruck auf dem falschen, in einer anderen Abteilung stehenden Drucker, sind hier zu nennen.

PDF statt Word-Dokument

Die Frage, welche Daten zu schützen sind, zieht fast zwangsläufig die Frage nach sich, mit welchen Mitteln Unternehmen unerlaubte Datenabflüsse verhindern. Heutzutage können bereits viele Produkte (E-Mail-Gateways, HTTP-Proxies) Policies durchsetzen, die etwa den Datenaustausch mit externen Kommunikationspartnern über Office-Dokumente verbieten. Diese Policies sind sinnvoll, da Office-Dokumente häufig Metadaten mit internen Informationen wie Autor, Speicherort des Dokuments oder Änderungshistorien enthalten. Häufig setzen Anwenderunternehmen deshalb für den externen Datenaustausch PDF- statt Office-Dateien ein. Wie lässt sich aber verhindern, dass über einen grundsätzlich zur externen Kommunikation zugelassenen Dokumenttyp wie PDF vertrauliche Daten aus dem Unternehmen transportiert werden?

Hier beginnt der Bereich der DLP-Produkte, die durch eine Analyse der Daten unterscheiden, welche vertraulich sind und welche nicht. Dazu untersuchen sie sowohl den Zusammenhang beziehungsweise Kontext, in dem die Daten auftreten, als auch deren Inhalt. Der vertrauliche Daten anzeigende Kontext ist für jeden Datentyp individuell verschieden. Eine E-Mail kann beispielsweise schützenswert sein, wenn sie der Vorstand an die Bank sendet, eine Datei etwa, wenn sie auf dem Server der Entwicklungsabteilung abgelegt ist.

Die Analyse kann vertrauliche Inhalte auf verschiedene Weise erkennen. Eine Variante ist das Beschreiben sensibler Inhalte über Schlüsselwörter und reguläre Ausdrücke (Code zur Beschreibung von Zeichenmustern). Die Verantwortlichen definieren dazu typische Schlüsselwörter und reguläre Ausdrücke und versehen sie mit einer entsprechenden Gewichtung. Gilt es beispielsweise eine neu entwickelte chemische Verbindung zu schützen, werden die Namen und Formeln der Ausgangs- und Endstoffe erfasst. Überschreitet die Summe der gewichteten Auftrittshäufigkeiten einen Schwellwert, so klassifiziert das System das Dokument als vertraulich.

Dieses Beispiel lässt aber auch ahnen, wie schwierig es ist, die vertraulichen Inhalte zu beschreiben, da die für die chemische Verbindung verwendeten Ausgangsstoffe ebenso in anderen, nicht vertraulichen Dokumenten vorkommen können. Ebenso wenig ist das Auftauchen der chemischen Formel des geheimen Endstoffs signifikant, da beispielsweise die Verbindung mit der Formel C_2H_6O sowohl Ethanol (CH_3-CH_2-OH) als auch Dimethylether (CH_3-O-CH_3) darstellen kann. Generell erfordert eine hohe Genauigkeit in der Erkennung sensibler Inhalte bei gleichzeitig geringer Falscherkennungsrate einen großen Aufwand bei der Erstellung des Regelwerks von Schlüsselwörtern und regulären Ausdrücken.

Eine weitere Technik der Inhaltsanalyse ist das sogenannte Fingerprinting, bei dem der Hash-Wert eines Dokuments gebildet wird. Ein Hash-Wert ist das Ergebnis einer mathematischen Funktion, die aus Eingabedaten unterschiedlicher Länge eine praktisch eindeutige Ausgabe kurzer, fester Länge erzeugt. Der Ausgabewert

ändert sich selbst bei minimaler Variation der Eingabe stark, sodass der Hash-Wert das vollständige, unmodifizierte Dokument repräsentiert und zu dessen Identifikation dienen kann. (Bekannte Hash-Algorithmen sind MD5 und SHA-1.)

Diese Methode erzeugt zwar keine falsch-positiven Ergebnisse, ist jedoch nicht resistent gegen einfachste Änderungen des Dokuments. Um auch Teile eines vertraulichen Dokumentes identifizieren zu können, unterstützen manche Lösungen das partielle Fingerprinting. Dazu bildet der Algorithmus Hash-Werte von vielen kleinen, einander überlappenden Teilen des Dokuments. Anhand dieser partiellen Hashes lassen sich selbst Teile eines vertraulichen Dokuments erkennen. Diese Technik funktioniert in der Regel sehr gut. Die zu markierenden Teile sollte man jedoch nicht zu klein wählen, da sonst eine allgemeingültige, häufig anzutreffende Phrase leicht zu falsch-positiven Ergebnissen führen kann.

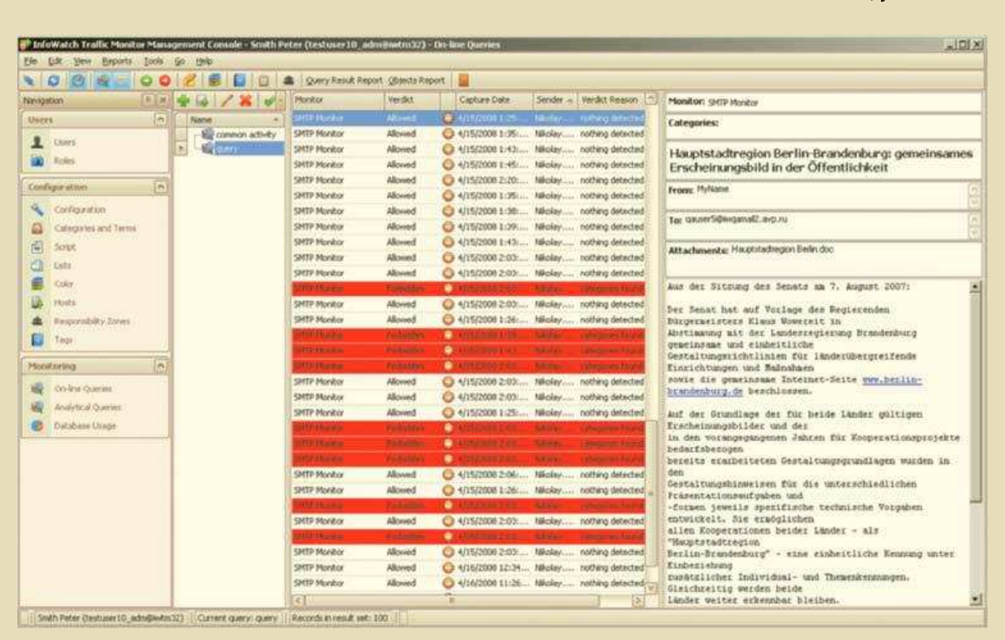
Für die Auswahl eines geeigneten DLP-Produktes sind nicht nur technische, sondern auch administrative Parameter zu berücksichtigen. Auf technischer Seite muss ein Unternehmen entscheiden, ob ein netzwerk-, ein agentenbasierter Ansatz oder beide zur Erfüllung der Anforderung erforderlich sind.

Weiterhin ist zu überlegen, wie die im spezifischen Umfeld relevanten Datenabflusskanäle etwa USB-Schnittstellen, Copy & Paste oder HTTP überwacht werden können. Dazu müssen die Verantwortlichen verbotene Vorgänge in ihren technischen Abläufen analysieren und mittels der Policy abbilden. Hierbei ist es erforderlich, sowohl den Inhalt der vertraulichen Informationen als auch den erlaubten Kontext klar zu definieren.

Legt ein Unternehmen durchgängig alle geheimen Daten in einem bestimmten Verzeichnis auf dem Fileserver ab, so ist der erlaubte Kontext für diese Daten schlicht eben dieses Verzeichnis auf dem Dateiserver. Jeden Versuch, die Daten nun an einen anderen Ort zu kopieren, unterbindet die Policy. Was aber geschieht, wenn ein Anwender diese Daten beispielsweise per USB-Stick transportieren muss? In diesem Fall lässt sich der erlaubte Kontext um die verschlüsselte Ablage der Daten auf diesen Datenträger erweitern. Dieses Vorgehen versagt jedoch immer dann, wenn aufgrund gewachsener Strukturen keine derartig eindeutige Zuordnung zwischen Kontext der Daten und umzusetzender Sicherheitsrichtlinie möglich ist. In diesem Fall hilft es nur, vertrauliche Daten zusätzlich über eine Inhaltsanalyse zu identifizieren.

Das Erstellen der Policy erfordert somit eine Kenntnis der Geschäftsprozesse, der Inhalte der Daten sowie die Fähigkeit, diese Parameter in entsprechende technische Nutzungsrichtlinien zu übersetzen. Hierbei sollten Verantwortliche darauf achten, verschiedene Administratorenrollen mit unterschiedlichen Rechten zu definieren. Der Ersteller dieser Nutzungsrichtlinien sollte etwa aus datenschutzrechtlichen Gründen keine Berechtigung zum Sichten der Logs und Reports haben, die Revision dagegen keinerlei Rechte zur Änderung dieser Policies. Erstrebenswert ist in diesem Fall eine Umsetzung nach dem Vier-Augen-Prinzip.

Die Revision kann die Vorfälle zwar einsehen, jedoch nur in anonymisierter Form. Erst bei Vorliegen eines konkreten Verdachts erhält sie durch Eingabe eines weiteren, nur dem Betriebsrat vorliegenden Passworts Zugriff auf die vollständigen, nicht anonymisierten Auswertungen. Da die detektierten Vorgänge strafrechtliche Relevanz erhalten können, bieten manche Produkte zusätzlich forensische Hilfen wie Audit Trails an. Diese Mechanismen ermöglichen es, unerlaubte Zugriffe, Datenabflüsse, Löschungen, Änderungen und Manipulationen an Dokumenten, Unterlagen oder anderen Aufzeichnungen nachzuvollziehen.



Die alarmrote Anzeige an der Managementkonsole des Produkts von Infowatch sollte den Systemverantwortlichen aufmerken lassen: Hier versucht jemand, vertrauliche Inhalte per Mail aus dem Unternehmen zu schleusen (Abb. 4).

Datenschutz nicht vernachlässigen

Da DLP-Produkte den Mitarbeiter weitreichend kontrollieren können, ist in Deutschland ihr Einsatz in der Regel von der Zustimmung des Betriebsrates abhängig. Aus betrieblicher Sicht ist es kaum möglich, eine „wasserdichte“ Policy zu entwickeln und dauerhaft zu betreiben, ohne den Anwender zu stark in seinen täglichen Abläufen zu behindern. Richtlinien sollten sich vielmehr darauf beschränken, nur die wirklich kritischen Aktionen mit den wirklich wichtigen Daten zu reglementieren.

Auch technisch gibt es Grenzen, speziell bei der Inhaltsanalyse (s. S. VIII). Vergleichsweise einfache Modifikationen der zu schützenden Daten wie das Austauschen etwa aller Buchstaben A eines Textes durch ein X reichen meist aus, um eine Analyse der Inhalte auszutricksen. DLP hilft den Unternehmen vor allen Dingen effektiv bei der Bekämpfung des fahrlässigen Umgangs mit vertraulichen Daten. Dem technisch versierten Anwender kann der Missbrauch der Daten zwar erschwert, aber nur selten komplett unmöglich gemacht werden. (sf/ur)

Sven Gerlach
ist Senior Consultant bei Integralis.



Securing Your Web World

Konzentrieren Sie sich auf die wirklich wichtigen Dinge!

Mehr Sicherheit für Ihre Daten? Mit Trend Micro steuern Sie mittels zentraler Managementkonsole mehrschichtige Sicherheitslösungen sowie Hosted Services, die Ihr Netzwerk proaktiv schützen.

Mit anderen Worten: Sie haben wieder mehr Zeit für die wirklich wichtigen Dinge, wie Business-Applikationen, Investitionsplanung oder sei es, mal wieder an einer Konferenz teilzunehmen, um sich Anregungen und wertvolle Informationen aus erster Hand zu holen.

BESUCHER

Security Summit 2008 "Wirtschaftsspionage"

Mit Trend Micro



KOSTENFREIE Testversionen und WERTVOLLE Tipps unter www.trendmicro.de/big

Dosierter Schutz

Techniken und Methoden zur Klassifizierung von Daten

Um den lese- und schreibberechtigten Nutzern sensibler Daten eine lästige Vollsperrung diverser Hardwareschnittstellen zu ersparen, statten Hersteller ihre sogenannten Data-Leakage-Prevention-Produkte mit Methoden zur Klassifizierung von Daten aus. Dabei versuchen sie festzustellen, ob eine Datei schützenswerten Inhalt enthält oder nicht.

Mittlerweile setzt sich in den Unternehmen die Erkenntnis durch, dass im Gegensatz zu gewohnten Datenschutzansätzen nicht die eingesetzten Systeme, sondern die vorhandenen Daten das zu schützende Gut sind. Techniken und Methoden zum Schutz der Systeme existieren in vielfältiger Form und die Unternehmen nutzen sie auf unterschiedliche Art und Weise. Da jedoch mit diesen klassischen Ansätzen ein Abfließen der Daten nicht – oder nur sehr schwer – verhindert werden kann, waren neue Lösungen notwendig.

Unbeliebte Vollsperrung

Die ersten Ansätze beschränkten sich zum Beispiel auf das Sperren der vorhandenen USB-Schnittstellen der Notebooks oder Desktop-Systeme. Dadurch wurde auf wirksame Weise ein Datenabfluss über externe Festplatten oder USB-Sticks verhindert. Doch war diese Variante nicht nur unflexibel, auch war sie bei den Benutzern sehr unbeliebt. Diese „Ganz oder gar nicht“-Ansätze brachten neben der geringen Akzeptanz der Benutzer den Nachteil mit sich, dass sie auch aus administrativer Sicht ausgesprochen starr waren.

Data Leakage Prevention (DLP) versucht auf intelligente Art festzustellen, ob eine Datei schützenswerten Inhalt enthält oder nicht. Grundsätzlich ergeben sich bei der weiteren Betrachtung der Datenanalyse drei Fragen: An welcher Stelle werden die anfallenden Daten gesammelt? Hier lassen sich die zwei Varianten netzwerk- oder hostbasierte Produkte beziehungsweise eine hybride Lösung unterscheiden (siehe Artikel „Abgedichtet“ auf Seite I). Nur mit einer hostbasierten Lösung können Unternehmen neben dem Netzwerk weitere Schnittstellen wie USB, CD/DVD, Zwischenablage und Ähnliches kontrollieren.

Die zweite Frage bezieht sich auf die drei Zustände der Daten:
– „Data in Motion“: Hier ist eine Kontrolle aller in Bewegung befindlichen Daten erforderlich, zum Beispiel Versand einer E-Mail oder FTP-Upload;
– „Data in Use“ benötigen eine Überwachung aller Formen der Dateioperationen wie Lesen, Schreiben, Kopieren, Verschieben;
– „Data at Rest“: Hier kommt eine relativ neue Überwachung aller Speicherorte der Daten zum Einsatz.

Schließlich geht es bei der dritten Frage um die möglichen Varianten der Überprüfung. Diese begrenzen sich auf die zwei Ansätze Kontext (Context) und Inhalt (Content) der Dateien.

Wer verschiebt was wohin?

Eine Kontextüberprüfung umfasst die Überwachung von Speicherquellen oder Speicherzielen, die Analyse von Metadaten oder Zeitstempeln sowie die Betrachtung von Dateitypen. Verschiebt jemand beispielsweise ein PDF-Dokument von Fileserver 1 auf eine externe USB-Platte von Host 2, erfolgt die Überprüfung, ob dieser Kopiervorgang legitim ist, auf Basis der Analyse von Datenquelle, -typ und -ziel. Auf diese Art erreicht man zwar eine effektive Form der Überwachung und Analyse des Datenstroms, Informationen über den Inhalt der Daten erhält man so allerdings nicht. Diese Form der Überwachung ist daher kaum ausreichend.

Um tatsächlich den Inhalt von Dateien zu betrachten und zu bewerten, greifen alle DLP-Produkte auf eine Analyse des Inhalts (Content Analysis) zurück. Dabei sind jedoch einige Besonderheiten und sogar Tücken zu beachten. Die eingesetzten Analysemodule der Produkte müssen in der Lage sein, den Inhalt der Dateien zu parsen. Das ist bei einer einfachen Textdatei noch eine überschaubare Herausforderung, schwieriger gestaltet sich der Vorgang bei komplexen Dokumenten, die darüber hinaus noch komprimiert und gepackt sind. Sollte zum Beispiel in einer mit ZIP gepackten Powerpoint-Präsentation eine Excel-Tabelle eingefügt sein, so müsste das eingesetzte Produkt in der Lage sein, die Datei zu entpacken, Powerpoint korrekt zu parsen, die eingefügte Tabelle zu entdecken und auch deren Inhalt korrekt zu analysieren.

Besonders schwierig gestaltet sich die Inhaltsanalyse jedoch bei verschlüsselten Dateien. Hier ist eine Analyse nur möglich, wenn entweder auf dem Host oder im Netzwerk eine Art Recovery Key existiert, der erlaubt, erst die Datei zu entschlüsseln und dann die oben beschriebene Analyse durchzuführen. Sinnvollerweise müssen also die eingesetzten DLP-Produkte neben den Standardformaten wie PDF, Office-Formaten, Packformaten wie RAR, ZIP und Ähnlichen auch die besonderen Dateiformate unterstützen, die in einer bestimmten Organisation eingesetzt werden. Darüber hinaus muss das Produkt sprachunabhängig sein, wenn es ebenfalls im multinationalen Umfeld Verwendung findet.

Um die eingangs erwähnte Vollsperrung der Schnittstellen zu vermeiden, bedarf es also intelligenter Techniken zur Analyse des Inhalts der vorhandenen Daten. Im Wesentlichen kommen sechs Verfahren zur Analyse des Inhalts von Dateien zum Einsatz. Die meisten Hersteller verwenden für ihre Produkte eine Kombination verschiedener Vorgehensweisen.

Am Anfang war der reguläre Ausdruck

Reguläre Ausdrücke bilden die klassische Form der Analyse und sind in allen DLP-Produkten im Einsatz. Diese erste Stufe der Analysetechnik dient der Erkennung fester Muster, wie sie in Adressen, Kreditkartennummern oder Postleitzahlen enthalten sind. In der Regel erweitern die Hersteller die einfache Form der regulären Ausdrücke, zum Beispiel über



CPI EAGLE BLADE 6306

EIN EINFACHES, FLEXIBLES UND PREISLICH ATTRAKTIVES SYSTEM

Der auf Intel® Multi-Flex Technology aufbauende **CPI Eagle Blade 6306** integriert Speicher, Server und Netzwerk, und vereinfacht so das komplexe IT-Umfeld.

Das flexible und leistungsfähige Serversystem **CPI Eagle Blade 6306** mit unterbrechungsfreier Installation, nahtloser Migration, skalierbarem Wachstum - eben ein Unternehmen im Kleinformat, ideal für kleine und mittelständische Unternehmen.

Leistungsfähige Funktionen:

- Skalierbare Server-Rechnerkapazität mit neuesten Intel® Xeon® Prozessoren
- Virtueller, integrierter, gemeinsam genutzter Speicher (hochverfügbares SAN)
- Einfache Verwaltung über die Virtual Presence-Benutzeroberfläche
- Ausfallsicherheit durch doppelt ausgelegte Komponenten
- Gemeinsame Anbindung über Ethernet und SAS

CPI Computer Partner Handels GmbH
Kapellenstr. 11
D - 85622 Feldkirchen/München

Telefon +49 (0)89 - 96 24 41 - 0
Telefax +49 (0)89 - 96 24 41 - 33
Hotline 0800 - 100 82 69
E-mail sales@cpigmbh.de

CPi server&storage

www.cpigmbh.de

die weitergehende Betrachtung von N-Grammen oder die linguistische Verarbeitung. Das Ziel ist, den Zusammenhang von Schlüsselwörtern zu verstehen und ihn in einen sinnvollen Kontext zu setzen.

Der Datenbank-Fingerabdruck ist eine Technik, die entweder über Onlineabfragen der Datenbank oder die Nutzung kompletter, zuvor erstellter Datenbank-Dumps zur Anwendung kommt. Ein Einsatzgebiet ist zum Beispiel die Überprüfung, ob Kundennamen oder Kundennummern aus der Datenbank in Dokumenten auftauchen.

Die Technik der exakten Datenübereinstimmung über Hash-Summen stellt im Prinzip eine Art Integritäts-Check à la Tripwire – vielen als Werkzeug zum Systemcheck bekannt – dar. Dabei werden Hash-Summen mit MD5 oder SHA über eine Datei gebildet und diese dann durch das DLP-Produkt analysiert und verglichen. Geht es um die Betrachtung statischer Dateien, so ist dies eine effiziente Methode, bei sich verändernden Office-Dateien jedoch ist dieses Verfahren sinnlos.

Herausforderung „Copy & Paste“

Eine weitere Methode besteht in der Prüfung der Übereinstimmung von Teilbereichen. Besonders wichtige Dokumente lassen sich über eine Analyse des kompletten Dokuments oder von Teilbereichen überprüfen, denn es besteht die Möglichkeit, dass Benutzer vertrauliche Inhalte in kleine Häppchen unterteilen und in eigene Dokumente kopieren. Die Teilanalyse ist jedoch sehr aufwendig, da die zu untersuchenden Segmente des Dokuments mit einem Hash versehen werden, den das System überprüfen muss. Die meisten Hersteller nutzen an dieser Stelle ebenfalls die Möglichkeit linguistischer Verarbeitung.

Statistische Analysen bieten mithilfe von gängigen statistischen Methoden – zum Beispiel Bayessche Statistik – eine Lernmöglichkeit. Statistische Methoden lassen sich bei unstrukturierten und unbekannten Daten sinnvoll einsetzen, bergen aber dadurch ein hohes Fehlalarm-Risiko.

Neuerdings liefern immer mehr Hersteller von DLP-Systemen vordefinierte Regelsätze und Wörterbücher mit, welche die Einhaltung behördlicher Auflagen wie GLBA (Gramm-Leach-Bliley Act sind Regularien der Finanzdienstleistung), SB 1386 (Richtlinien für die Vertraulichkeit persönlicher Informationen) und SOX unterstützen. Für die PCI-Compliance, die Einhaltung des neuen Sicherheitsstandards der Kreditkartenindustrie (siehe Artikel „Schutzzwang“ in diesem Heft) werden immer die Muster der Kreditkartennummer abgefragt. Zu diesem Zweck gibt es vorgefertigte Module und Parser, die den Aufbau der Nummer schon kennen, Gleiches gilt für SB 1386.

Hier sind die interessanten Werte Sozialversicherungsnummer, Kreditkartennummer, Adresse et cetera. Sie sind ebenfalls im Modul vordefiniert. Die einzelnen Kreditkartennummern, Sozialversicherungsnummern und weitere Daten des Unternehmens sind nicht in Modul oder Search Engine hinterlegt, wohl aber die Struktur. Im Wesentlichen ist dieses Modul eine deutliche Erleichterung für die Administratoren. Sollte ein Unternehmen nach den obigen Nummern suchen wollen, könnte es das Regelwerk SB 1386 anwenden und müsste nicht eigene Filter und Module bauen.

Für den deutschen Markt ist, bis auf das Regelwerk EU Data Protection Directive, der Markt noch eher dünn. Grundsätzlich können die Hersteller aber auch hier alles „vorbauen“, was der Markt an Compliance bietet. Der Vorteil hier liegt im deutlich geringeren Implementierungsaufwand durch maßgeschneiderte Regelsätze. Vor- und Nachteile der unterschiedlichen Methoden zur Inhaltsanalyse beziehungsweise Klassifizierung zeigt die gleichnamige Tabelle.

Fazit

Für gewöhnlich nutzen alle Hersteller eine Kombination aus Kontext- und Inhaltsanalyse in ihren Produkten. Zur Inhaltsanalyse werden die oben aufgeführten Techniken in Teilen oder als Mischform genutzt. In Summe bieten die DLP-Produkte eine sinnvolle Möglichkeit, den Datenabfluss aus dem Unternehmen zumindest teilweise zu kontrollieren. Leider können auch die besten DLP-Produkte nicht verhindern, dass der Benutzer den Bildschirm mit seiner im Handy eingebauten Kamera abfotografiert – bei Hunderten von Kundendatensätzen dürfte ihm aber zumindest der Spaß daran und am späteren Abtippen vergehen. (sf/ur)

Jörg Schäfer
ist IT-Sicherheits-Consultant bei der Berliner HiSolutions AG.

VOR- UND NACHTEILE DER KLASSIFIZIERUNGSMETHODEN

Methode	Vorteil	Nachteil
reguläre Ausdrücke	sehr guter Eingangsfilter, kann Standardwerte wie Kreditkartennummern abfangen, mächtige Konfigurationsmöglichkeiten	viele Fehlalarme („False Positives“)
Datenbank-Fingerabdruck	sinnvoller Einsatz in Verbindung mit Datenbanken	hohe Belastung für das Produkt bei großen Datenbanken, Belastung für die Datenbank bei häufigen Abfragen
exakte Datenübereinstimmung über Hash-Summen	kann auf einfache Art für alle Dateitypen genutzt werden	bei sich verändernden Daten sinnlos, da neue Hash-Summe
Übereinstimmung von Teilbereichen	für ausgewählte, wichtige Dokumente wie Geschäftsbericht sinnvoll	erfordert präzises Wissen, welche Dokumente zu schützen sind/„False Positive“-Rate kann hoch sein
statistische Analyse	bei unstrukturierten und unbekannten Daten sinnvoll	viele Fehlalarme
Vorlagen für Kategorien	sehr gut für definierte Kategorien nutzbar	nicht sinnvoll, außerhalb der Kategorie erweiterbar



Klare Vorteile für KMUs, Konzerne und Service Provider

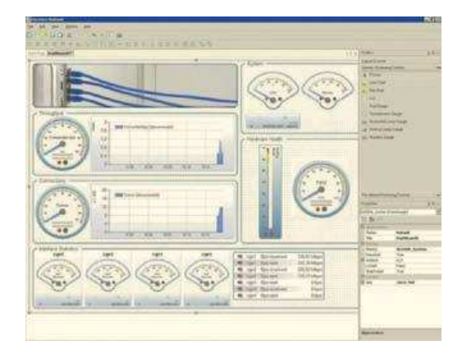
Managed Security Services

Der Markt für Managed Security Services wächst beständig, jedoch galt es als schwierig und kostenintensiv, diese Dienstleistung im Outsouring-Verfahren zu erbringen. Clavisters neue Security Service-Plattform beseitigt diese Probleme und ermöglicht es so Resellern, Systemhäusern, IT-Abteilungen sowie Service Providern effizient auf dem Outscouring-Security-Markt zu agieren.

Die Clavister Security Service-Plattform (SSP) steht für das gesamte Clavister-Produktportfolio von Security-Gateways, UTM-Appliance- sowie Management Systeme und den damit zusammenhängenden Sicherheits-Services. Diese Lösung, kombiniert mit den Clavister Lifecycle-Systemen FineTune, PinPoint, und Insight setzt einen neuen Standard für Managed Security Services, da sich einerseits die Total Cost of Ownership (TCO) auf ein Minimum reduzieren lässt und andererseits ein rascher Return of Invest (ROI) erreichen lässt: sowohl für KMUs, die ihre Security an externe Dienstleister auslagern, als auch für Konzerne, die über interne IT-Serviceabteilungen verfügen und Service Provider, die ihren Kunden wiederum Sicherheitsdienstleistungen anbieten wollen. FineTune und PinPoint werden von Clavister kostenlos angeboten, wodurch Manage Security Service Provider im Gegensatz von herkömmlichen Lösungen massiv Geld sparen können. Die Hardware-Basis in den Zentralen bilden dabei UTM-Appliance-Systeme der 4000er-oder 3000er-Systemreihen. Zur Anbindung von Niederlassungen kommt die SG10-Serie zum Einsatz. Die SG10-Serie garantiert Manage Security Service Providern eine optimale und sichere Anbindungen von kleinen Firmen oder Außenstellen. Damit werden Kompromisslösungen vermieden, die Service Provider in der Vergangenheit dazu gezwungen hatten sich zwischen Standardprodukten mit unzureichenden Funktionen oder teuren Lösungen mit unnötig vielen Features zu entscheiden. Die SG10-Serie bietet darüber hinaus noch weitere Vorteile: Beispielsweise kann eine Antivirus Scan-Engine und eine Supportfunktion für Clavisters InSight Reporting- und Logfile-Analyse-System integriert werden. Ebenso enthält die Serie eine Web Content Filtering-Funktion sowie ein Intrusion Detection und Prevention (IDP/IPS) System.

Die Lösung ermöglicht einen schnellen und kosteneffizienten Einsatz der Managed Security Services (MSS), beispielsweise in den Bereichen:

- Managed VPN
- Managed Wireless Network Protection
- Managed Firewalling
- Managed Intrusion Detection and Prevention (IDP)
- Managed Antivirus Protection
- Managed Content Filtering
- Managed Web-Use Reporting
- Managed Regulatory Compliance Reporting



Die Clavister SSP-Plattform zeichnet sich durch die Fähigkeit aus, sich an das Wachstum der Unternehmen anpassen zu können (Clavister xPansion Lines). Hierzu wurde die Lösung mit Feinabstimmungsmechanismen und hochgradig skalierbaren Funktionen ausgestattet, die es jedem Betreiber ermöglichen, diese an seine individuellen Leistungs- und Funktionsanforderungen nahtlos anzupassen. Die Tatsache, dass sowohl der Clavister SSP als auch das Customer Premise Security Gateway (CPE) dasselbe hoch skalierbare Betriebssystem Clavister CorePlus™ verwenden, macht jegliche Kompromisse zwischen maximalem Service, Verfügbarkeit, Funktionalität, Steuerbarkeit, TCO sowie Kapitalinvestitionen hinfällig.

Mit **FineTune** steht den Anbietern von Managed Security Services ein modernes, graphisch orientiertes Management-System (GUI) zur Verfügung, das die zentrale Verwaltung einer Vielzahl von Clavister Security-Gateways aus einer benutzerfreundlichen GUI-Umgebung heraus, ermöglicht. Über dieses Management-System ist die Remote-Verwaltung aller Clavister-Devices inklusive deren Konfiguration, Real Time-Monitoring sowie -Logging, Revisionskontrolle und Firmware Upgrades möglich und wird via 128-Bit-Verschlüsselung und Authentifizierungsmechanismen effektiv geschützt.

Mit **Clavister-PinPoint™** ist ein neues Tool verfügbar, mit dem Sicherheitsprozesse in Echtzeit überwacht werden können. Dieses ermöglicht Security Managern über eine intuitiv zu bedienende Oberfläche einen grafischen Überblick u.a. über Surfgewohnheiten, Resultate von Virus- oder Malware-Scans, Einbruchsversuche in das Netzwerk oder VoIP-Statistiken. Vergleichbar mit einem Flugzeug-Cockpit, können die „Piloten“ von PinPoint essenzielle Daten (Mission Critical) von weniger wichtigen (Non-Critical) unterscheiden und anzeigen lassen. Clavister ist der erste Hersteller, der eine einfach zu bedienende Applikation auf den Markt bringt, die Security-abhängige Vorfälle in Echtzeit visualisiert.

Durch **Clavister InSight** wird diese Plattform mit erweiterten Funktionen für das Logging und Monitoring von Security-Events und um umfassende Alarm- und Forensikfunktionen ergänzt. InSight bietet eine leistungsfähige „Security-Intelligenz“, die automatisch alle Event-Daten von Clavister-Systemen und anderen Multi-Vendor-Netzwerkgeräten wie Router oder Switches etc. sammelt, kontrolliert und reportet. InSight liefert folgende fortschrittliche Security-Intelligence-Features wie zum Beispiel: GUI (Graphical User Interface)-basierter detaillierter Event-Drilldown, User-definierbare Event- und Threat-Level-Klassifizierung, Heterogenes Real-Time-Monitoring, zusammengefasstes Reporting und viele weitere wertvolle Funktionen.

Auch wenn die Firmen noch zögern, insgesamt mehren sich die Anzeichen dafür, dass sich der MSS-Markt in einem Aufschwung befindet. Das zeigt die Umsatzentwicklung der europäischen Security-Outsourcing-Anbieter: Die Analysten von Gartner bescheinigen diesen eine durchschnittliche jährliche Wachstumsrate von 14,9 Prozent.

CLAVISTER™
Deutschland
Tel.: +49 40 411259-0
E-Mail: info@clavister.de · www.clavister.de

Sichern Sie sich den preiswerten Umstieg auf Ihre Clavister-SSP-Plattform!

Nur im Juni und Juli 2008! Clavister gewährt im Rahmen seines TradeIn-Programms einen Rabatt von 10 Prozent bei der Ablösung alter Firewallsysteme durch die Clavister-SSP-Plattform.
Bitte melden Sie sich bei uns unter info@clavister.de oder telefonisch unter: +49 40 4112950

Bewusstseinserweiterung

Best Practices bei der Umsetzung von Data Leakage Prevention

Nicht immer schleusen Mitarbeiter aus purer Bösartigkeit oder für einen guten Nebenverdienst Daten aus dem Unternehmen, häufig genug mangelt es an Problembewusstsein oder technischem Verständnis. Die Einführung von Data Leakage Prevention im Unternehmen soll vor allem der Sensibilisierung dienen und das Arbeiten so wenig wie möglich behindern.

Data-Leakage-Prevention-Produkte (DLP) gibt es in allen möglichen „Geschmacksrichtungen“ und von den unterschiedlichsten Herstellern. Zum einen existieren netzwerkbasierte DLP-Systeme, die mit speziellen Algorithmen den Datenstrom auf Policy-Verletzungen untersuchen. Auf der anderen Seite stehen hostbasierte Lösungen, die einen Agenten für die Einhaltung der Unternehmens-Policies auf dem Endgerät einsetzen. Zusätzlich gibt es hybride Systeme, die gleichzeitig Sensoren im Netz und Agenten einsetzen und deren Ergebnisse miteinander korrelieren können.

Bei den Policies gibt es ebenso viele unterschiedliche Herangehensweisen. Beim Einsatz von kontextbasierten Systemen lässt sich definieren, was mit Dateien geschehen soll, die an einem bestimmten Ort gespeichert sind oder die an einen anderen Ort kopiert werden sollen. Beispielsweise könnte man das Kopieren vom Netzlaufwerk auf den lokalen PC stillschweigend erlauben, jedoch beim Kopieren auf einen USB-Stick eine Warnung an den Benutzer ausgeben, dass es sich dabei um ein potenziell unsicheres Medium handelt.

Einen anderen Ansatz verfolgen inhalts- oder contentbasierte Produkte. Sie suchen nach frei definierbaren Mustern in Dateien oder Datenströmen. Damit ließe sich beispielsweise erkennen, dass eine ausgehende Mail Kreditkarteninformationen, Stichwörter wie „vertraulich“, „Übernahme“ oder auch die direkte Kombination zweier Wörter wie „Jahresabschluss“ und „Deckungsbeitrag“ enthält.

Im kleinen Kreis Erfahrungen sammeln

Welcher Ansatz besser für ein Unternehmen geeignet ist, hängt eng mit dem geplanten Einsatzgebiet zusammen. In der Praxis ist es eher unwahrscheinlich, dass ein DLP-Produkt in einem Zug unternehmensweit ausgerollt wird. Vielmehr beginnt man häufig mit einem eingeschränkten Benutzerkreis, der mit besonders wichtigen und vertraulichen Daten umgeht. Die damit gewonnenen Erfahrungen lassen sich dann in weiteren Schritten für den Rest des Unternehmens verwerten.

Als konkretes Anwendungsbeispiel kann ein Unternehmen im Bereich der Softwareentwicklung dienen. Die Firma möchte sich kurz vor der Fertigstellung eines neuen Produkts davor schützen, dass illoyale Mitarbeiter den Quellcode aus der Organisation mitnehmen und an die Konkurrenz verkaufen. Eine mögliche Lösung wäre der Einsatz eines DLP-Produkts, das das Kopieren von Quellcode auf USB-Medien, CDs, FTP-Server und so weiter verhindert.

Ein ganz anderer Anwendungsfall ergibt sich etwa im Vorstandsbereich eines börsennotierten Unternehmens. Ein Mitarbeiter hat in diesem Bereich Zugang zu höchst vertraulichen Informationen wie Finanzdaten, Prognosen, Übernahmeplänen et cetera. Hier könnte eine DLP-Lösung zum Einsatz kommen, die die Mitarbeiter im bewussten Umgang mit diesen Informationen unterstützt. Beispielsweise könnte das System um eine Begründung bitten, wenn Mitarbeiter vertrauliche Daten auf ihren PC oder ein externes Medium kopieren möchten.

Eine weitere denkbare Option ist eine automatische Verschlüsselung der Zieldatei nach dem Kopiervorgang, sodass sie nur noch innerhalb der DLP-Umgebung lesbar ist. Eine verlorene oder an die Konkurrenz verkaufte CD wäre somit wertlos.

Nicht böswillig, sondern leichtfertig

Insbesondere wenn es um den Umgang mit Personendaten, Kreditkartennummern oder Informationen mit Börsenrelevanz geht, ist die Unterstützung beziehungsweise Sensibilisierung von Mitarbeitern die wichtigste Funktion eines DLP-Produkts. Denn nur in den wenigsten Fällen ist das Abfließen von Daten auf ein zielgerichtetes, böswilliges Verhalten zurückzuführen.

Sowohl die Aussagen und Umfragen von Herstellern als auch die Erfahrungen der Anwender zeigen, dass ein großer Teil von Indiskretionen erfolgt, weil Mitarbeiter kein ausreichendes Sicherheitsbewusstsein und technisches Verständnis für den Umgang mit vertraulichen Daten haben. Viele Unternehmen setzen DLP-Produkte daher lediglich zu dem Zweck ein, ihre Mitarbeiter gezielt zu unterstützen und schrittweise zu erziehen. Sicherheitsvorkehrungen wie straffe Dateisystemrechte, Festplattenverschlüsselung oder Device-Blocker sind im Vergleich zu DLP-Systemen schlicht machtlos, wenn ein Mitarbeiter eine vertrauliche Datei per E-Mail an seinen privaten Account schickt, um in bester Absicht nach Feierabend weiterarbeiten zu können.

Ein zentraler Aspekt bei der Einführung von DLP ist die Auswahl und Lokalisierung der Informationen, die einen besonders hohen Wert für das Unternehmen haben. Gerade in Betrieben, die über mehrere Jahre hinweg oder durch Zukäufe gewachsen sind, stellt sich das häufig als äußerst schwierig heraus. Zum einen liegen Daten möglicherweise über unzählige Fileserver verstreut, zum anderen ist es mitunter knifflig, den eigentlichen Besitzer von Dateien oder Verzeichnissen zu benennen. Die Abteilung, die eine DLP-Lösung einführen soll, steht hier vor der Frage, mit was für einer Art Daten und mit welcher Vertraulichkeitsstufe sie es überhaupt zu tun hat.

Um Schwierigkeiten bei der Lokalisierung und Klassifizierung vertraulicher Informationen auszuräumen, bieten die führenden DLP-Produkte integrierte Mechanismen, die auf sämtlichen Endgeräten und Servern Dateien erfassen und

kategorisieren. Dazu werden die vorhandenen DLP-Agenten auf Clients und Dateiservern genutzt. Sie helfen, Dateien beim Zugriff oder auch periodisch zu klassifizieren.

Metainformationen separat gespeichert

Wie beschrieben arbeiten viele Produkte inhaltsbasiert, um Muster und Schlagwörter innerhalb von Dateien zu suchen. Außer Kreditkarteninformationen oder Kundennummern et cetera kann man damit auch Sourcecode finden, der etwa an Schlagwörtern wie „public static void“ oder weiteren Schlüsselwörtern erkennbar ist.

Die Zuordnung erfolgt an der Datei selbst, ein möglicher Mechanismus ist etwa die Speicherung der Klassifikation in den sogenannten Alternate Data Streams des NTFS-Systems. Das bietet den Vorteil, dass die Datei durch die Klassifizierung selbst nicht verändert wird.

Anwendungsgebiete für eine derartige inhaltsbasierte Klassifizierung finden sich in Unternehmen, in denen Dateien über viele Dateiserver verstreut sind oder in denen es darum geht, eine erste Übersicht über die Verteilung und die Vertraulichkeit der eigenen Daten zu erhalten. Die Ergebnisse lassen sich mitunter als Grundlage für eine Policy verwenden oder um bisherige Strukturen und Prozesse unter Sicherheitsaspekten aufeinander abzustimmen.

Eine ganz andere Art der Klassifizierung führen spezielle Data-Governance-Produkte durch. Sie können über einen Agenten auf den Dateiservern über jede Datei herausfinden, welche Personen und Abteilungen tatsächlich täglich mit den Daten arbeiten beziehungsweise sie erstellen. Das Ziel dabei ist, genau den Personenkreis abzuleiten, der am besten über Inhalt und Vertraulichkeit der Dateien entscheiden kann.

Vorsicht vor Datenschutzverstößen

Ein weiterer zentraler Punkt, über den sich Anwender schon weit im Vorfeld einer Einführung Gedanken machen sollten, ist das Logging des DLP-Produkts. Die meisten der heutigen Produkte sind in der Lage, nicht nur Verstöße gegen Unternehmens-Policies zu protokollieren und zu verhindern, sondern detailliert jede Dateioperation, jeden URL-Aufruf und alle E-Mail-Operationen zu protokollieren, die ein Benutzer durchführt. Bei einigen dieser Produkte ist diese implizite Protokollierung sogar standardmäßig voreingestellt.

Die Mehrzahl der derzeit am Markt verfügbaren Produkte kommt nicht aus Deutschland, sondern etwa aus Amerika oder Israel. Hier gelten andere Gesetze für den Umgang mit mitarbeiterbezogenen Daten, teilweise ist dort sogar eine Protokollierung der Tätigkeiten der Mitarbeiter und ihres täglichen Arbeitsverhaltens erwünscht. In Deutschland können DLP-Systeme mit Features zur allumfassenden Überwachung jedoch in Konflikt mit dem Bundesdatenschutzgesetz (BDSG) und Mitarbeiterüberwachungsparagrafen (z. B. BetrVG § 87, Abs. 1 Nr. 6) kommen.

Um frühzeitig Konflikte aus dem Wege zu räumen, ist eine enge Abstimmung und Betrachtung unter rechtlichen Aspekten nötig. Ein detailliertes Rollen- und Administrationskonzept, das etwa die Szenarien „täglicher Betrieb“ und „Forensik“ klar voneinander trennt, kann Missbrauch verhindern. Für den Administrator im täglichen Betrieb wären in dem Fall lediglich die einzelnen Agenten, Trends und anonyme Zusammenfassungen sichtbar. Im Fall des Verdachts, dass vertrauliche Dateien das Unternehmen verlassen haben, können die Verantwortlichen in enger Zusammenarbeit mit dem Betriebsrat den Zugang zu sämtlichen Detaildaten erlangen.

DLP soll Arbeit nicht blockieren

Geht es um den Entwurf einer Policy für ein DLP-Produkt, setzen die Verantwortlichen selten im ersten Schritt eine Policy ein, die Aktionen des Benutzers gezielt verhindert. Vielmehr wird zu Beginn lediglich das bisherige Verhalten eines Mitarbeiters erfasst, gegebenenfalls werden Warnungen an ihn ausgegeben. Anhand der gewonnenen Erkenntnisse lässt sich die Policy sukzessive anpassen.

Möglicherweise erkennt man so aber auch Schwachpunkte in den etablierten Geschäftsprozessen. Wenn Mitarbeiter es beispielsweise gewohnt sind, vertrauliche Informationen per unverschlüsselter Mail zu versenden, sollten die Verantwortlichen das als Anlass sehen, nach den Ursachen für dieses Verhalten zu suchen und es zu ändern. Dennoch ist ein DLP-Produkt im Idealfall für den Benutzer transparent beziehungsweise gänzlich unsichtbar. Das bedeutet, dass der DLP-Agent im Hintergrund bleibt und den Benutzer nicht behindert, solange dieser nicht gegen die Regel verstößt.

Je nach Zielsetzung des Unternehmens empfehlen sich für eine Policy unterschiedliche Herangehensweisen. Häufig kommt es darauf an, einen eleganten Kompromiss zwischen Sicherheit und Aufrechterhaltung des Betriebs zu finden. Zum einen sollen Benutzer nicht unnötig in ihrer täglichen Arbeit eingeschränkt werden, die Alarme durch das DLP-System nicht zu sehr zunehmen und der Helpdesk soll nicht durch Anrufe verärgerter Benutzer überlastet werden. Zum anderen muss man die Sicherheit der Daten durch Einschränkung der potenziellen Datenbewegungen maximieren.

Heutige DLP-Produkte sind deutlich flexibler als Device-Blocker, die durch Blockieren der Schnittstellen die Benutzung von USB-Geräten, Netzwerk-Interfaces oder Ähnlichem gänzlich verhindern. Die Policies lassen sich granularer einstellen. Beispielsweise kann ein DLP-System beim Kopieren auf USB-Medien aufgrund der Herkunft oder Klassifizierung zwischen vertraulichen und öffentlichen Daten unterscheiden. Außerdem bieten sie eine Vielzahl an Reaktionen im Fall einer Policy-Verletzung.

Die Palette reicht von stiller Protokollierung über Warnmeldungen an den Benutzer bis hin zu Formularen, in denen ein Benutzer eine Rechtfertigung für den ausgeführten Vorgang eingeben muss. In jedem Fall lässt sich einstellen, ob die

Auch „sanfte Maßnahmen“ wie Warnhinweise senken die Anzahl der Policy-Verstöße bereits signifikant. Schon die Ankündigung über den Einsatz eines DLP-Produkts lässt die Zahl der Verstöße abnehmen und den Benutzer bewusster agieren (Abb. 1).

Ihre PCs brauchen:

- Sicherheit an allen Schnittstellen
- Kontrolle aller Devices, Medien und Dateien
- Data Loss Prevention (DLP)
- Automatische Verschlüsselung
- Medienbasierte Sicherheit
- Personalisierte Datenträger
- Applikations-Kontrolle
- Awareness der Benutzer

Alles aus einer Hand
Kosteneffizient
Sicher!

DLP mit PDWatch

Firmenschlüssel - Daten bleiben in der Firma:

Verschlüsselung kann mit persönlichen Schlüsseln oder einem Firmenschlüssel erzwungen werden: für bestimmte Dateien nach Namen und/ oder Inhalt benutzer- und gruppenspezifisch. Firmenschlüssel sind nur auf Firmenrechnern verwendbar und verhindern den Datendiebstahl. VIP-User verwenden den Firmenschlüssel optional. Datenlecks werden geschlossen – erlaubte Dateibewegungen protokolliert XRayWatch.

Compliance durch content-sensitive Verschlüsselung:

Das BDSG§9 verlangt beim Speichern personenbezogener Daten auf mobilen Datenträgern höheren Schutz. Unsere „Zwangsverschlüsselung" erfüllt diese Anforderung. Protokollierung und die Zustimmung des Anwenders sind automatisierte Echtzeit-Prozesse. Unkritische Daten bleiben unverschlüsselt. VIP-User haben alle Rechte - der Haftungsübergang wird bei Bedarf protokolliert.

Mehr Infos dazu unter **www.itWatch.de/PDWatch.pdf**

Null Administration - Volle Sicherheit:

Das aktuelle White Paper finden Sie im Netz unter **www.itWatch.de/NullAdmin_VolleSich.pdf**



itWatch GmbH
Tel.: +49 89 620 30 100
info@itWatch.de
www.itWatch.de



Benutzeraktion erlaubt oder verboten sein oder ob die Zieldatei sogar transparent verschlüsselt werden soll. Grundsätzlich bieten DLP-Systeme gegenüber Device-Blockern Optionen, Einschränkungen und Verbote an geeigneten Stellen zu lockern und dem Benutzer dadurch mehr Flexibilität zu bieten, ohne die Sicherheit gleich komplett auszuhebeln.

Kleine Maßnahmen – große Wirkung

Unabhängig von der gewählten Policy und den Logging-Fähigkeiten können Anwender während der konkreten Einführung einer DLP-Lösung beziehungsweise eines Pilotversuchs interessante Nebeneffekte beobachten. In den USA wurde beispielsweise während einer solchen Einführungsphase die Entwicklung des Benutzerverhaltens untersucht. Ziel war herauszufinden, inwieweit das Wissen über den Einsatz eines solchen Systems das Benutzerverhalten beeinflusst.

Dabei stellten die Forscher fest, dass allein die Benachrichtigung über den Einsatz eines Produkts, das das Verhalten von Benutzern protokollieren kann, Auswirkungen hatte. Die Beobachtungen ergaben, dass sich mit der Bekanntmachung die durchschnittliche Anzahl der Policy-Verstöße um einen beachtlichen Prozentsatz verringerte (Abbildung 1). Die Verstöße gingen nach der Einführung von Warnhinweisen, die die Benutzer auf Verstöße aufmerksam machten, weiter zurück.

Ein derartig umfassender und tiefgreifender Eingriff in Geschäftsprozesse wie bei DLP ruft natürlich immer Kritiker auf den Plan, die die Software hinterfragen oder versuchen, Lücken und Schwachstellen im System zu finden. Auf der organisatorischen Seite kommen häufig Fragen nach Betrieb und Verantwortlichkeit sowie der gefürchteten Überwachung.

Doch wie oben dargestellt, wählen viele Unternehmen die Methode der sukzessiven Anpassung der Policy, die zu Beginn nur passiv im Hintergrund protokolliert. Auf diesem Weg lässt sich der anfängliche Betriebsaufwand relativ gering halten. Ist eine Policy etabliert und haben sich die Benutzer an die Interaktion mit einem DLP-System gewöhnt, sind an den Policies üblicherweise keine Veränderungen mehr vorzunehmen.

Die Verantwortlichkeit für das System hängt unter anderem von der gewählten Technologie ab. Netzwerkbasierte DLP-Systeme sind in anderen Bereichen anzusiedeln als hostbasierte Systeme. Zudem haben Erstere den Nachteil, dass sie wegen der eingeschränkten Sichtweise und Heuristiken Fehlalarme produzieren können, die der Verantwortliche periodisch auswerten muss. Hostbasierte Systeme dagegen können direkt am Ursprung des Vorfalls ansetzen und liefern daher erfahrungsgemäß zuverlässigere Ergebnisse.

Technische Aspekte berücksichtigen

Auf der technischen Seite gibt es häufig Fragen, wie tief sich DLP-Agenten in das Betriebssystem der Clients einklinken. Um Benutzervorgänge wie Kopieren von Dateien, Drucken, Speichern, Bildschirmausdrucke oder Netzwerkkommunikation kontrollieren zu können, ist eine Einbettung in den Kernel nötig. Deshalb müssen vor Implementierung und Patch-Rollout – wie auch bei anderen Softwareprodukten üblich – Kompatibilitätstests durchgeführt werden, um Wechselwirkungen mit anderen lokalen Produkten auszuschließen.

Ebenso stellen sich viele die Frage, wie sich derartige Systeme umgehen lassen. Menschen mit genügend krimineller Energie und Fachwissen werden sicherlich einen Weg finden, trotz DLP-Agent vertrauliche Daten aus dem Betrieb oder der Behörde zu schleusen. Häufig hängt das damit zusammen, wie der Kompromiss zwischen Sicherheit und Produktivität gewählt ist. Doch selbst wenn ein böswilliger Mitarbeiter einen Weg finden sollte, mit technischen Tricks vertrauliche Daten zu kopieren, so wird er in der Regel zumindest so viele Spuren hinterlassen, dass sich der Weg zu ihm zurückverfolgen lässt.

Grundsätzlich haben viele Unternehmen eingesehen, dass es nicht darum geht, sich hundertprozentig und vor sämtlichen Missetätern zu schützen, sondern dass man mit heutigen DLP-Systemen einen Großteil an Datenbewegungen oder -abflüssen kontrollieren und die Mitarbeiter in der täglichen Arbeit mit vertraulichen Daten unterstützen und sensibilisieren kann. (sf/ur)

Max Ziegler
ist Consultant bei der Heilbronner cirosec GmbH.

In iX extra 8/2008:

Storage – Management für Speichernetze

Schlagworte gibt es viele in der Speicherbranche. Doch wie sehen die Auswirkungen von Datenwachstum, Compliance oder Konsolidierung für die Speicherinfrastruktur und die Speichernetze wirklich aus? Damit die IT-Abteilung der Entwicklung nicht einfach hinterherläuft, sollte sie ihre Überwachungs- und Verwaltungstools auf dem neuesten Stand halten. Ein Reality-Check muss sich um den Stand der Dinge bei LAN, SAN und NAS kümmern: Wird Fibre Channel over Ethernet (FCoE) Fibre Channel und iSCSI ablösen? Zurück zu einem Netz für alles?

iX extra wirft ferner einen Blick auf Virtualisierung als Management-Instrument für Storage, automatische Lastverteilung und Ressourcen-Management und vergleicht die großen Management-Suites. Last, but not least: Was ist eigentlich aus der groß angekündigten Initiative der SNIA geworden, mit SMI-S einen Standard für Storage Management zu entwickeln?

Erscheinungstermin:
24. Juli 2008

DIE WEITEREN IX EXTRAS:

Ausgabe		Thema	Erscheinungstermin
09/08	Networking	Load Balancing	21.8.08
10/08	Embedded Systems	Echtzeit- und eingebettete Betriebssysteme	18.9.08
11/08	IT-Security	Sicherheitsmanagement durch Appliances	16.10.08